ЦТРК100503.112779.ПЗ-16

Оценка эффективности принятых мер защиты информации в информационной системе персональных данных коммерческой организации

Студент группы КТСО _____

ФИО

Руководитель Басан А.С.

Цель и задачи

Основной целью данного дипломного проекта является разработка методики оценки эффективности принятых мер по защите персональных данных в коммерческой медицинской организации, для решения данной цели были решены следующие задачи:

- анализ законодательной базы России в области защиты персональных данных, применительно к коммерческой медицинской организации;
- исследование существующей информационной системы персональных данных коммерческой медицинской организации, изучение ее системы защиты и принятых организационных мер;
- разработка методики проведения оценки эффективности принятых мер;
- применение методики к существующей информационной системе коммерческой медицинской организации и анализ полученных результатов;
- устранение выявленных недостатков, разработка системы защиты, удовлетворяющей требованиям законодательства России.

Описание существующей информационной системы

- наличие разнородного системного программного обеспечения, в частности операционных систем семейства Windows: Windows Server 2012 R2, Windows XP, Windows 8.0, Windows 8.1, Windows 7 Professional, Ubuntu Desktop Edition;
- наличие одного сегмента сети, где обрабатываются персональные данные;
- наличие серверного программного обеспечения, реализующего технологию «клиент-сервер» для ведения бухгалтерии, баз данных пациентов и сотрудников, а также регистрации и ведения истории болезни пациентов;
- наличие выхода в глобальную сеть в «Интернет».

Определение перечня персональных данных

- Персональные данные медицинских работников
- Персональные данные остальных сотрудников
- Персональные данные клиентов

Законодательство :

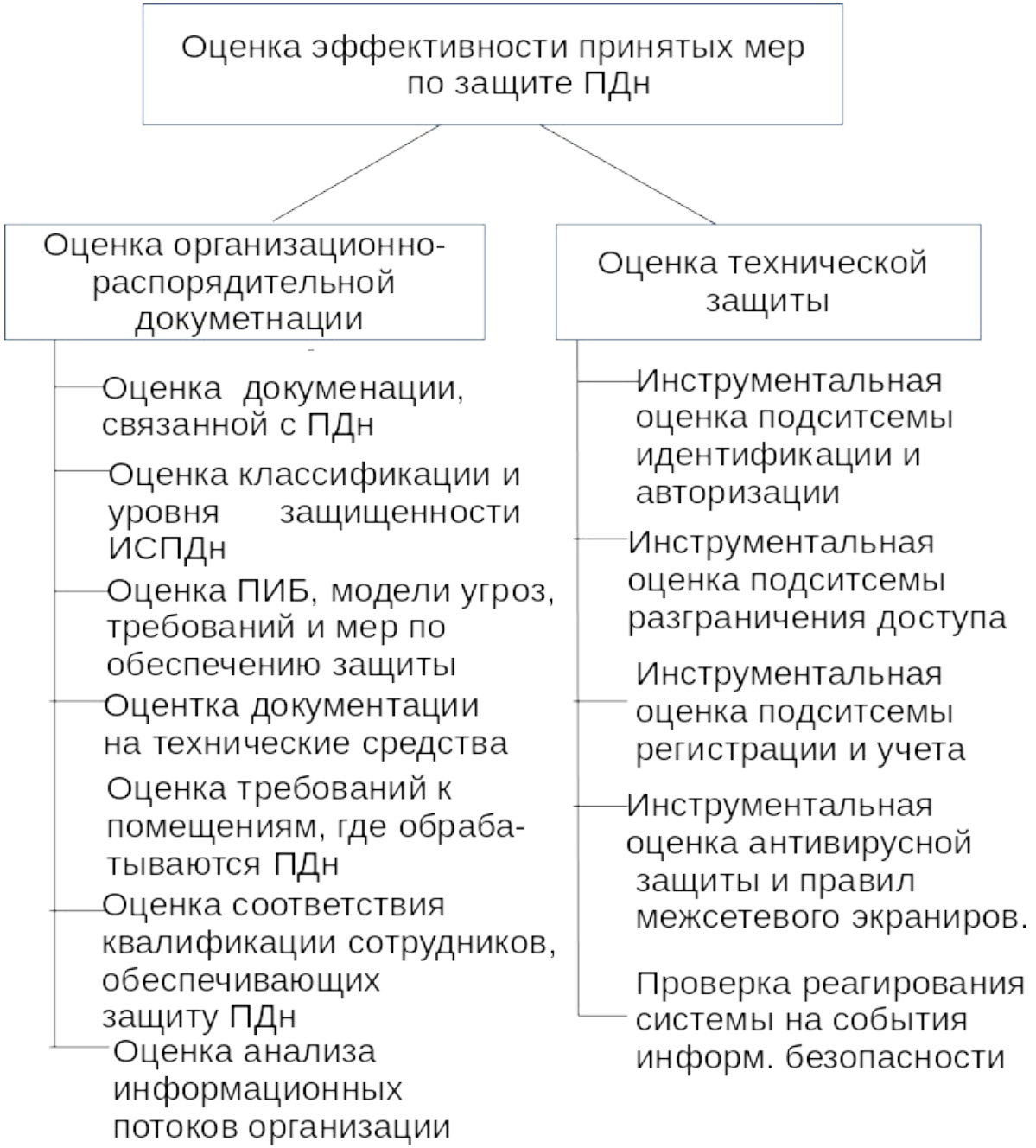
- «Трудового кодекса РФ»;
- Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 N 323-ФЗ;
- «Налогового кодекса Российской Федерации (часть вторая)» от 05.08.2000 N 117-ФЗ,
- Федерального закона от 01.04.1996 N 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федерального закона от 24.07.2009 № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;
- Постановления Госкомстата РФ от 05.01.2004 N 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».

Определение уровня защищенности персональных данных

- 1. Информационная система персональных данных «Медицина +» является информационной системой, обрабатывающей специальные категории персональных данных, так как в ней обрабатываются персональные данные, касающиеся состояния здоровья субъекта персональных данных.
- 2. Для ИСПДн «Медицина +» актуальными являются угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.
- 3. ИСПДн «Медицина +» обрабатывает специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.
- В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в автоматизированной информационной системе персональных данных «Медицина +» медицинской коммерческой организации необходимо обеспечить 3-й уровень защищенности персональных данных.

Описание выбранных средств защиты

Разработка общей концепции проведения оценки эффективности



Разработка этапа оценки организационно-распорядительной документации

1 Оценка документации, связанной с ПДн

1.1 Проверка целей обработки ПДн

1.2 Проверка законности обработки персональных данных

1.3 Проверка сроков обработки ПДн

2 Оценка политики информационной безопасности

2.1 Обоснованность выбора типа нарушителя

2.2 Актуальность определенных угроз

2.3 Соответствие мер по защите

2.4 Обоснованность выбора состава и классов технических средств защиты

2.5 Наличие перечня защищаемых информационных ресурсов и матрица доступа к информационным ресурсам

2.6 Наличие инструкций и назначение ответственного за организацию процесс обеспечения защиты

2.7 Наличие нормативной и необходимой организационно-распорядительной документации

3. Оценка классификации и уровня защищенности ИСПДн

3.1 Наличие документа отражающего информацию о классификации

3.2 Правильность проведенной классификации

3.3 Оценка соответствия имеющихся технических средств и средств защиты информации, представленным в документации

3.4 Оценка выбранного для информационной системы типа актуальных угроз

Разработка этапа оценки организационно-распорядительной документации

4 Оценка документации на технические средства защиты
4.1 Наличие сертификатов соответствия ФСЭК
4.2 Наличие паспорта (формуляра) технического средства
4.3 Актуальность сертификата
4.4 Соответствие классу защищенности
5 Оценка требований к помещениям, где обрабатываются ПДн
5.1 Проверка режима доступа в помещения
5.2 Защита от считывания
6. Оценка соответствия квалификации сотрудников, обеспечивающих защиту ПДн
6.1 Проверка знания инструкций
6.2 Проверка документов
6.3 Проверка знания технологий
7 Оценка анализа информационных потоков
7.1 Содержание информационного потока
7.2 Соотнесение информационных потоков с внешними информационными системами и организациями
7.3 Законное основание передачи персональных данных

Разработка этапа оценки технической защиты

1 Сканирование персональных компьютеров системы

2 Инструментальная оценка подсистемы идентификации и авторизации

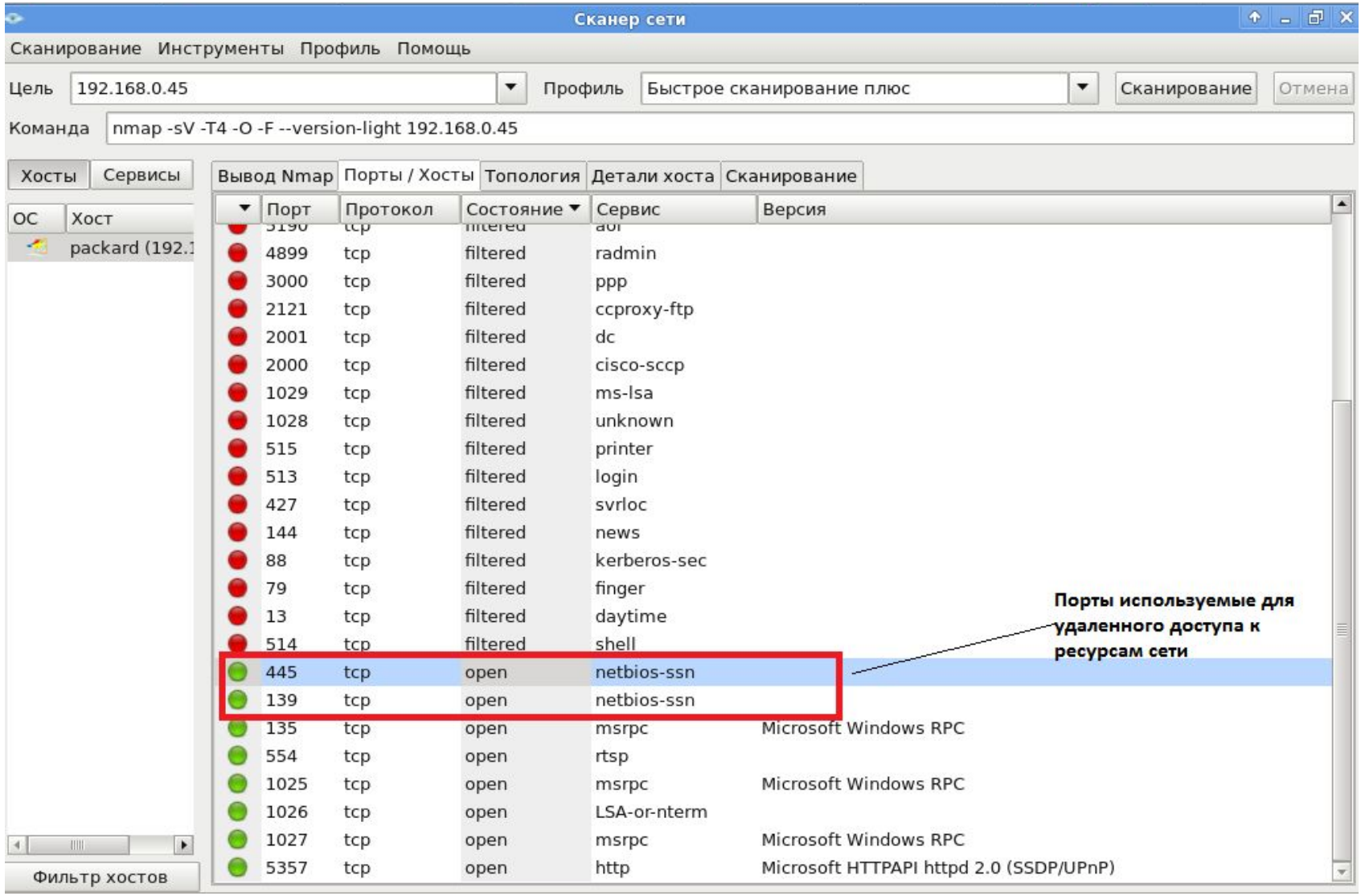
3 Проверка подсистемы разграничения доступа

4 Проверка подсистемы регистрации и учета

5 Проверка подсистемы антивирусной защиты и межсетевого экранирования

6 Проверка подсистемы реагирования на события безопасности

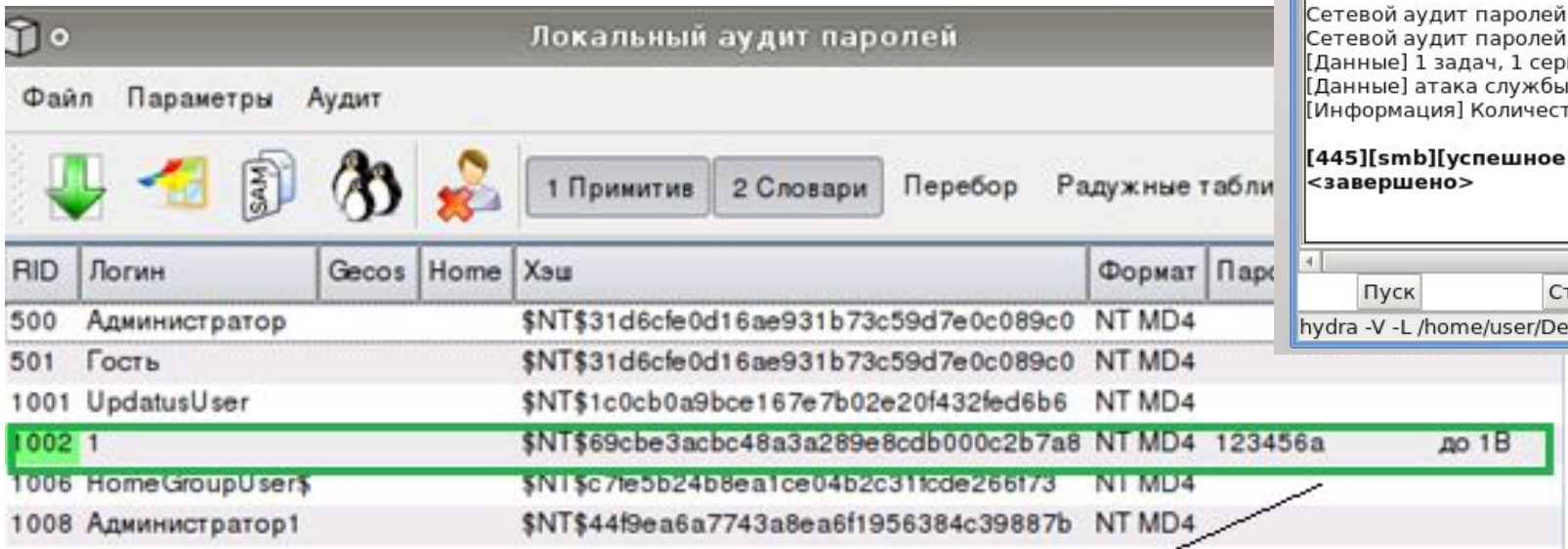
Инструментальная оценка подсистемы идентификации и авторизации



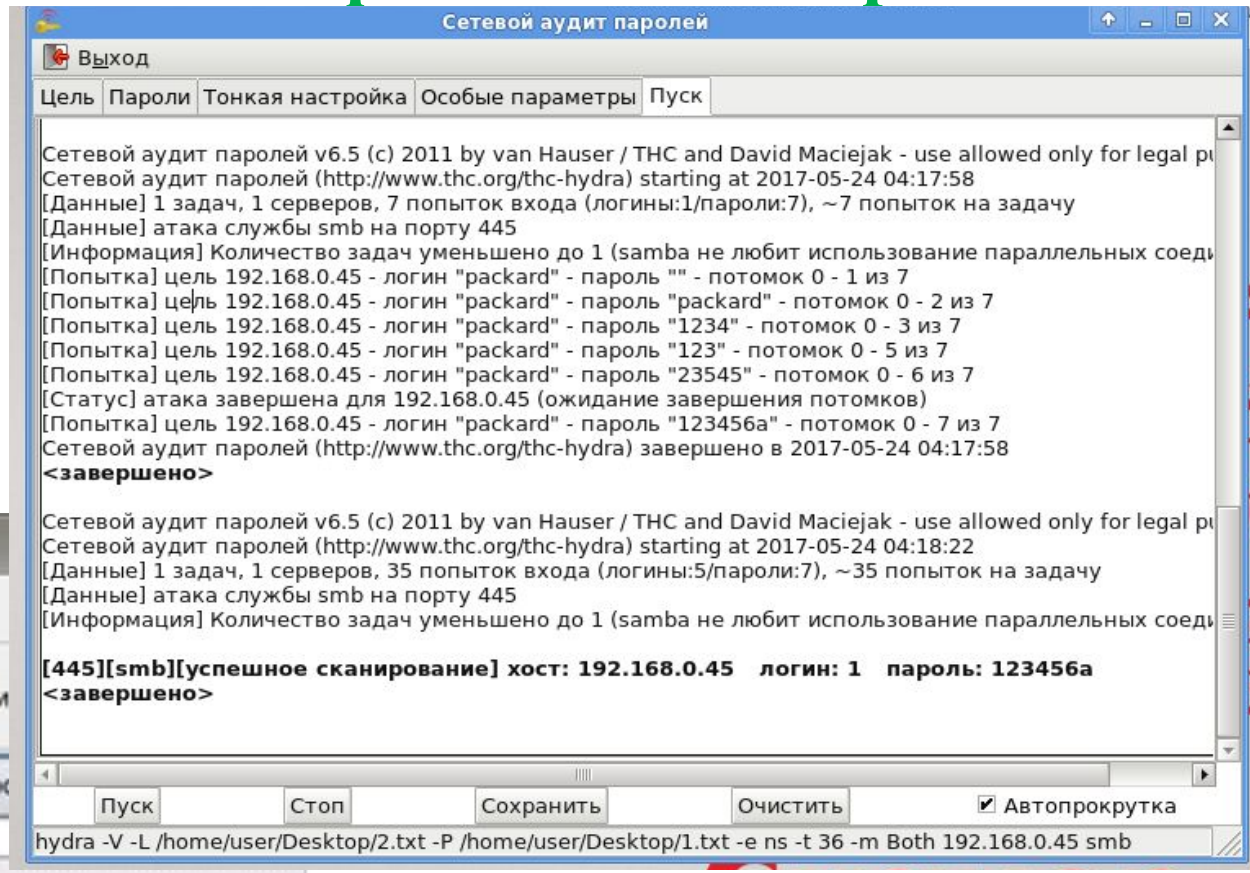
Сканирование портов узла системы

Инструментальная оценка подсистемы идентификации и авторизации

Локальный аудит паролей

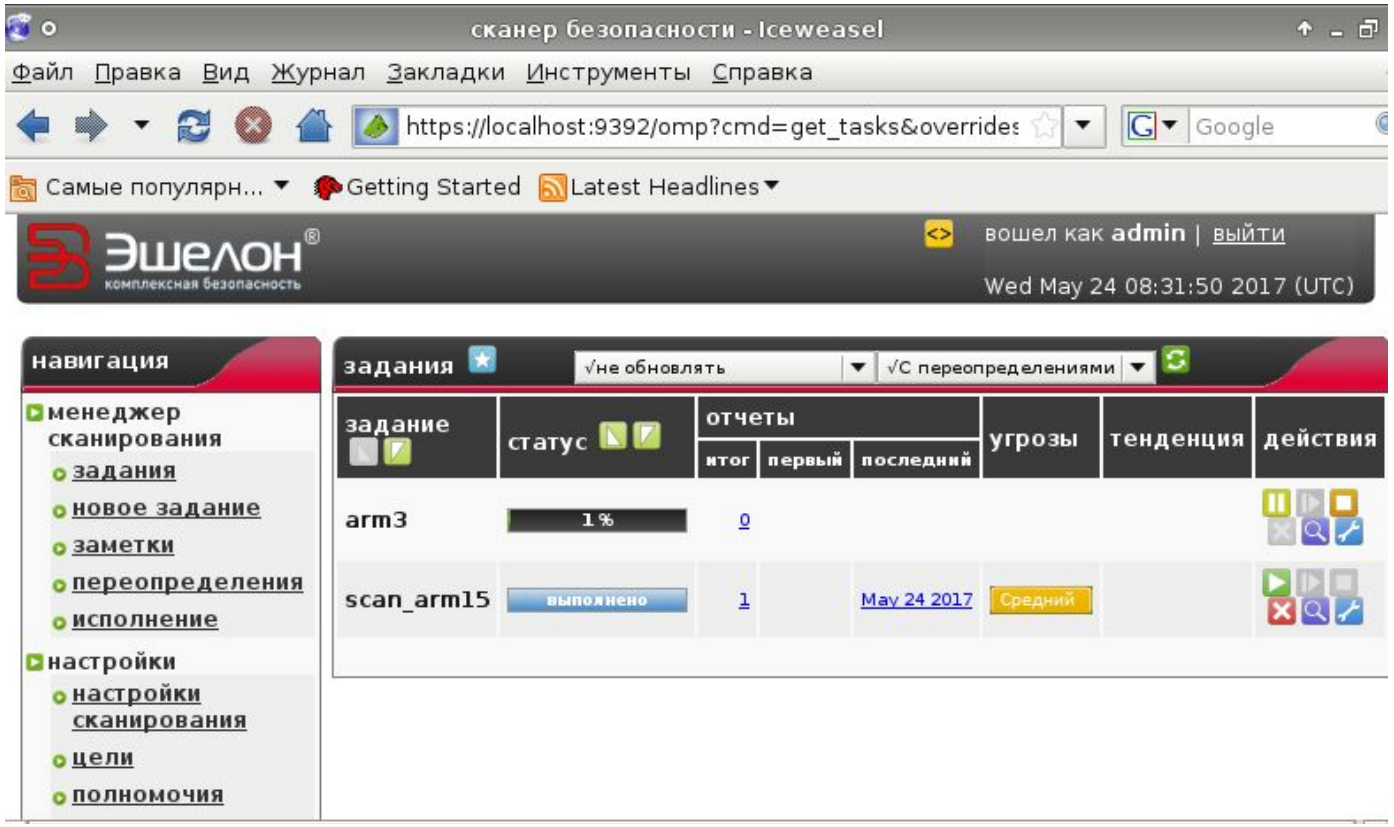


Найден пароль для пользователя с именем 1



Сетевой аудит паролей

Проверка подсистемы антивирусной защиты и межсетевого экранирования



Результаты сканирования портов узла 192.168.0.82

Сервис (Порт)	Уровень угрозы
netbios-ns (137/udp)	Medium
general/tcp	Low
icslap (2869/tcp)	Low
microsoft-ds (445/tcp)	Low
netbios-ssn (139/tcp)	Low
general/HOST-T	Log
general/SMBClient	Log
rtsp (554/tcp)	Log
ssh (22/tcp)	Log

Уязвимости безопасности узла 192.168.0.82

Medium netbios-ns (137/udp)
NVT: Использование NetBIOS для доставки информации от Windows-хоста (OID: 1.3.6.1.4.1.25623.1.0.10150)

```
Следующие 6 NetBIOS имена были получены :
 ALEXWIN7VIRT     = Это имя компьютера, зарегистрированное для сервисов WINS клиентом.
 WORKGROUP        = Рабочая группа / имя домена
 ALEXWIN7VIRT     = Имя компьютера.
 WORKGROUP        = Рабочая группа / имя домена (part of the Browser elections)
 WORKGROUP
   __MSBROWSE__
Удаленная хост-машина имеет следующий MAC-адрес на своем адаптере :
   08:00:27:6a:1a:f3
Если вы не хотите, чтобы каждый мог видеть NetBios-имя
вашего компьютера, вы должны фильтровать входящий трафик на этот порт.
Фактор риска : Средний
CVE : CAN-1999-0621
```

Результат сканирования целей «Сканером безопасности»

Отчет об уязвимостях Сканера безопасности

Применение разработанной методики на объекте информатизации. Проверка организационно-распорядительной документации

№	Этапы и пункты проверки согласно методике	Степень соответствия пунктам методики	Разъяснение
1.1	Проверка целей обработки ПДн	Частично соответствует	Недопустимая (излишняя) обработка ксерокопий документов
1.2	Проверка законности обработки персональных данных	Частично соответствует	Незаконное размещение информации о штатных сотрудниках в сети «Интернет»
1.3	Проверка сроков обработки ПДн	Не соответствует	Оператором не определены сроки обработки
2.4	Обоснованность выбора состава и классов технических средств защиты	Частично соответствует	Из-за ошибки в выборе уровня защищенности ИСПДН «Медицина +», класс выбранных средств защиты должен быть изменен согласно Приказу ФСТЭК №21
2.5	Наличие перечня защищаемых информационных ресурсов и матрица доступа к информационным ресурсам	Частично соответствует	Отсутствует матрица доступа, права сотрудников к защищаемым ресурсам не разграничены
3.2	Правильность проведенной классификации	Частично соответствует	С учетом роста количества субъектов персональных данных в системе, ИСПДН «Медицина +» должна иметь 2 класс защищенности.
3.3	Оценка соответствия имеющихся технических средств и средств защиты информации, представленным в документации	Частично соответствует	Имеющееся средство межсетевого экранирования не соответствуют требованиям приказа ФСТЭК № 21. Класс технических средств защиты должен быть изменен согласно новому уровню защищенности системы.

Проверка технической защиты информационной системы персональных данных

№	Этапы и пункты проверки согласно методике	Степень соответствия пунктам методики	Разъяснение
1	Сканирование персональных компьютеров системы	Частично соответствует	Сканирование выявило наличие открытых портов, которые несут угрозу информационной безопасности
2	Инструментальная оценка подсистемы идентификации и авторизации	Частично соответствуют	Отсутствует возможность контроля идентификации субъекта доступа при попытки получения сетевых ресурсов из-за отсутствия самой матрицы доступа.
3	Проверка подсистемы разграничения доступа	Частично соответствует	Доступ к сетевым ресурсам не разграничен из-за отсутствии матрицы доступа в ОРД
4	Проверка подсистемы регистрации и учета	Соответствует	-
5	Проверка подсистемы антивирусной защиты и межсетевого экранирования	Частично соответствует	Правила межсетевого экранирования некорректно настроены
6	Проверка подсистемы реагирования на события безопасности	Соответствует	-

Проверка подсистемы антивирусной защиты и межсетевого экранирования

Общий результат

Узел	Высокий	Средний	Низкий	Лог	Ложное срабатывание
192.168.0.45	0	2	22	26	0
Всего: 1	0	2	22	26	0

Результаты сканирования узлов

Узел 192.168.0.45

Сканирование узла началось: Wed May 24 09:04:37 2017
Количество найденных уязвимостей: 50

Результаты сканирования портов узла 192.168.0.45

Сервис (Порт)	Уровень угрозы
epmap (135/tcp)	Medium
netbios-ns (137/udp)	Medium
apex-mesh (912/tcp)	Low
blackjack (1025/tcp)	Low
cap (1026/tcp)	Low
exosee (1027/tcp)	Low
general/tcp	Low
iad2 (1031/tcp)	Low
icslap (2869/tcp)	Low
ideafarm-chat (902/tcp)	Low
lnvmailmon (2285/tcp)	Low
microsoft-ds (445/tcp)	Low
ms-lsa (1029/tcp)	Low
netbios-ssn (139/tcp)	Low
ratl (2449/tcp)	Low
rtsp (554/tcp)	Low
general/HOST-T	Log
general/SMBClient	Log
ssh (22/tcp)	Log

Medium epmap (135/tcp)
NVT: Переписывание служб DCE (OID: 1.3.6.1.4.1.25623.1.0.10736)

```
Распределенная среда обработки данных, запущенная на удаленной хост-машине,
может быть переписана посредством подключения к порту 135 и выполнения
соответствующих запросы.
Злоумышленник может воспользоваться этим для получения данных
об удаленной хост-машине.
Решение : фильтровать входящий через этот порт трафик.
Фактор риска : Низкий
```

Medium netbios-ns (137/udp)
NVT: Использование NetBIOS для доставки информации от Windows-хоста (OID: 1.3.6.1.4.1.25623.1.0.10150)

```
Следующие 3 NetBIOS имена были получены :
 PACKARD         = Это имя компьютера
 PACKARD
 WORKGROUP       = Рабочая группа / имя домена
Удаленная хост-машина имеет следующий MAC-адрес на своем адаптере :
   a8:54:b2:5b:88:c3
Если вы не хотите, чтобы каждый мог видеть NetBios-имя
вашего компьютера, вы должны фильтровать входящий трафик на этот порт.
Фактор риска : Средний
CVE : CAN-1999-0621
```

1 Результат сканирования системы на уязвимости. Открытые порты системы.

2 Результат сканирования системы на уязвимости. Разъяснение результатов

Выработка мер по устранению выявленных недостатков

Смета на закупку технических средств защиты.

Наименование	Кол-во	Цена, руб.	Сумма, руб.
Поставка средств защиты информации			
Сертифицированный ФСТЭК России межсетевой экран ALTELL NEO 100	1	86000	86000
Средство анализа защищенности "Сканер-ВС (специальная версия)"	1	6000	6000
Право на использование Средства защиты информации Панцирь-К	30	4000	120 000
		Всего	212 000

Оценка политики информационной безопасности:

Изменение класса средств защиты согласно новому уровню защищенности:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационно телекоммуникационными сетями международного информационного обмена.

Разработка документа, включающего в себя матрицу доступа к объектам защиты.

Необходимо определить перечень сетевых ресурсов, к которым необходимо ограничить доступ.

Правильность проведенной классификации:

- изменение класса защищенности ИСПДн с 3 класса на 2 класс;
- изменение классов технических средств защиты.

Предложенные меры по организации технической защиты ИСПДн «Медицина +»

1 В рамках обеспечения идентификации и аутентификации обладает следующими возможностями:

- Механизм авторизации, позволяющий подключать аппаратные средства ввода парольных данных (eToken и др.);
- Механизм контроля корректности идентификации субъекта доступа к ресурсам (контроль олицетворения).

2 Проверка подсистемы разграничения доступа.

- Механизмы разграничения доступа к локальным и разделенным в сети ресурсам – к файловым объектам, к объектам реестра ОС, к внешних накопителям, к принтерам, к сетевым хостам и др.;
- Механизм включения в разграничительную политику субъекта «процесс», как самостоятельного субъекта доступа к ресурсам, принципиально расширяющий функциональные возможности защиты и противодействующий атакам на расширение привилегий;
- Механизм управления подключением устройств.

3. Необходимо произвести корректную настройку правил межсетевого экранирования:

- ограничить доступ по уязвимым портам из внешней сети;
- реализовать сегментирование сети, задать правила доступа для каждого сегмента подсети;
- реализовать правила межсетевого экранирования согласно политике безопасности.

Основные полученные результаты

- 1. В рамках написания данного дипломного проекта была изучена структура информационной системы персональных данных «Медицина +», кроме того, была изучена документация, которая описывает принятые Оператором организационные меры, проанализирован состав документации, посвященной созданию системы защиты персональных данных, а также введению режима коммерческой тайны на предприятии.
- 2. Проведен анализ существующего законодательства Российской Федерации в области обеспечения безопасности персональных данных. выявлены основные моменты, на которые необходимо обращать внимание оператора при организации процесса обеспечения персональных данных.
- **3. Одним из основных результатов дипломного проекта является разработанная методика оценки эффективности принятых мер по обеспечению защиты персональных данных.** Особенностью данной методики является то, что подобная методика отсутствует в открытом доступе и коммерческие организации не могут использовать существующие решения для оценки своей системы защиты.
- 4. Были изучены функциональные возможности программного средства «Сканер-ВС» при проведении оценки эффективности принятых мер по защите.
- 5. Проведена проверка коммерческой медицинской организации с использованием разработанной методики. Данная проверка выявила ряд недостатков существующих мер по защите персональных данных.
- 6. Для устранения выявленных недостатков были предложены компенсирующие меры, включающие в себя меры для корректировки организационно-технической документации и меры по созданию новой технической системы защиты медицинской коммерческой организации.

Безопасность и экологичность проекта. Технико-экономическое обоснование

Наименование статьи калькуляции	Аналог Сумма, руб.	Разработка Сумма, руб.
Единовременные затраты	370450	235030
Текущие затраты на эксплуатацию изделия	0	0
Итого, интегральный стоимостный показатель (цена потребления)	370450	235030
Коэффициент цены потребления, Кэ=Ip/Ia	0.63	

Технические меры профилактики.

- входной контроль получаемого оборудования;
- использование передовых технологий, с минимизацией вредного влияния на окружающую среду и здоровье людей;
- соблюдение стандартов энергосбережения;
- использование качественных источников электропитания;
- помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации;
- соблюдение требований к эксплуатации и утилизации оборудования, также стандартов энергосбережения;
- использование сертифицированного оборудования и лицензионных программ.